



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/275,911	03/24/1999	ROBERT G. LIU	42390.P7033	1385

7590 06/10/2004

BLAKELY SOKOLOFF TAYLOR AND ZAFMAN
7TH FLOOR
12400 WILSHIRE BOULEVARD
LOS ANGELES, CA 90025

EXAMINER

BAUM, RONALD

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 06/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/275,911

Applicant(s)

LIU ET AL.

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 April 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,4-7,11-14,16,18-21,25,26,29,32,34 and 35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,4-7,11-14,16,18-21,25,26,29,32,34 and 35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 08 April 2004.
2. Claims 1,4-7,11-14,16,18-21,25,26,29,32,34 and 35 are pending for examination.
3. Claims 1,4-7,11-14,16,18-21,25,26,29,32,34 and 35 are rejected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1,4-7,11-14,16,18-21,25,26,29,32,34 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ibaraki et al, U.S. Patent 5,546,461, and further in view of Chapman, U.S. Patent 6,173,402 B1, and further in view of Faria, UK Patent Application GB 2316278A, and further in view of SCHNEIER, BRUCE, Applied cryptography, second edition, John Wiley & Sons, Inc. 1996, pages 193, section 9.3, 1st paragraph, IDS paper No. 4 as applied to claims 2 and 16 above, and further in view of, Dent, U.S. Patent 5,091,942.

As per claims 1,6,14,20, Ibaraki et al is directed towards an: "invention [that] relates to a scramble system for use in either a recording and reproducing system such as a digital video recorder or the like, or a transmission and receiving system for use through communication line such as an optical, coaxial or wireless communication line, in particular, to a scramble system comprising a scramble apparatus for scrambling a digital video signal and a descramble

Art Unit: 2136

apparatus for descrambling the scrambled digital video signal, wherein, in further particular, the scrambled digital video signal is transmitted through an optical, wire or wireless communication line, or the scrambled digital video signal is recorded into a recording medium such as a magnetic tape, a magnetic disk, a magneto-optical disk, a compact disk or the like.” (col. 1, Field of invention). Further: “The scramble unit 12 and the descramble unit 16 execute data processing by means of a block encryption. The block encryption is exemplified in, for example, U.S. Pat. No. 3,958,081, which utilizes the DES (Data Encryption Standard). This encryption is to encode and decode data in 64-bit blocks. In the encryption stage, a normal statement block is scrambled based on a key, thereby consequently obtaining an encryption block in 64 bits. On the other hand, in the decoding or deciphering stage, the encryption block in 64 bits is descrambled through reverse conversion of the scramble process based on the same key which is used in the encoding stage, thereby consequently restoring the normal statement block in 64 bits. The scramble unit 12 and the descramble unit 16 of the first preferred embodiment execute their processes by means of the DES.” (col. 13, lines 10- 24).

Ibaraki et al fails to teach of the use of the scrambling being responsive to a remote computer number.

Chapman teaches of: “A technique, system, and computer program for protecting data stored by a computer system in a computing environment having a connection to a public Network [i.e., the internet]. The stored data is created and accessed by a software application, which encrypts it for storing and decrypts it for processing. A secret, immutable value specific to the computer system [remote computer number] on which the software is running is combined with information identifying an authorized user in order to form the input key used by the

Art Unit: 2136

encryption and decryption facilities of the software. Optionally, the secret value can be exposed to the user in order to move the encrypted data to another environment.”(ABSTRACT)

It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Chapman teachings of the use of an immutable value specific to the computer system (remote computer number) for the keying in the scrambling (encryption) / descrambling (decryption) process, to the Ibaraki et al scramble system for digital video signal transmission / reception through a communication system, to allow secure data transmission through the system and prevent system compromise (via such mal-ware as viruses or Trojans).

Such motivation exists in the Chapman teachings concerning the specific reasons for the use of (at least partially) used key data that is not entered by the user, to account for Trojan malware that monitors keyboard keystroke input of user name or password data (col. 1, lines 49- 57).

Ibaraki et al and Chapman does not teach the use of logical exclusive OR'g (XOR) to create scrambling/de-scrambling data (Claims 1,6,14,20 additionally recite the limitation that logical exclusive OR'g (XOR) is used (an inherently 2 operand logical operation) to create scrambling/de-scrambling data from the data and another operand (the key in claims 6,20)).

Faria encrypts /decrypts by XOR of the data (1st operand) and the keying (other operand) data (page 3, lines 4-43, page 4, lines 1-14).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Faria teachings of the use of encrypting /decrypting by XOR'g of the data (1st operand) and the keying (other operand) data to the Ibaraki et al and Chapman encryption method in order to reduce the time consuming nature of

Art Unit: 2136

algorithmic transformation (encryption / encoding) of the (audio /video) data (Faria, page 2, lines 1- 4).

Faria is further directed towards a method of encrypting and subsequent decrypting sequences of bits (blocks of (streaming) data) comprising individually transforming (scrambling) the data blocks with a encryption key (page 2, lines 16-22). The user sends the server it's unique identity code (remote computer number), whereas the server also stores the audio and/or video data to be sent to the user (page 2, lines 27-38) as is done for MPEG audio and/or video (as per claims 4,5,18,19).

Therefore, the Faria encryption/decryption (scrambling/de-scrambling) of data is done on a received data file block of data (digital video) using a key that is a function of the receiver (remote computer) unique identity (number) code (page 2, lines 27-36).

Faria (and Ibaraki et al and Chapman) does not teach the use of data chaining of any given block of data with data from a previous block.

Schneier teaches that chaining adds feedback to block cipher: "The results of the encryption of previous blocks are fed into encryption of the current block..." (section 9.3, 1st paragraph). Also, where the feedback is the plaintext, Plaintext Block Chaining (PBC) is the encryption mode used (page 208, More Modes paragraph). In this case, the PBC initialization vector (page 194, Initialization paragraph) is the applicant's processed key, and each subsequent feedback input to the XOR function is the previous plaintext (digital video data) block. The chaining is done to prevent block replay of ECB encrypted data blocks (section 9.2, last paragraph).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the data block chaining of Schneier to the XOR scrambling of data blocks of Faria to prevent block replay attacks on the data block stream (Schneier, section 9.2, last paragraph).

The numbering of the digital video data blocks is determined and used as a component of the encryption/decryption key (claims 1,11,14 additionally recite such limitations). The Ibaraki et al, Chapman, Faria, and Schneier combination does not teach the use of the digital data blocks (data framing designation) being numbered.

Dent teaches of the use of a data frame to frame (block) determined number to generate the keystream data used for the stream encryption/decryption (col. 2, lines 67-68, col. 3, lines 1-14, col. 9, lines 16-22) via modulo-2 addition (XOR) operation (col. 11, lines 17-24).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Dent teachings of the use of data frame to frame (block) determined number to generate the keystream data used for the stream encryption/decryption (via the logical XOR operation on the operands) to the Ibaraki et al, Chapman, Faria, and Schneier combination encryption/decryption method for video/audio data streams. Dent describes how transmit to receive synchronization is a requirement for the communications to occur (col. 3, lines 3-10).

5. Claims 7,25 additionally recite the limitation that the remote computer number is the processor number. Chapman clearly discloses using the CPU serial number as the immutable characteristic (col. 12, lines 17- 21).

Art Unit: 2136

6. Claims 12,13 additionally recite the limitation that the remote computer number be used for authentication of the remote computer. Chapman clearly discloses authentication of the correct machine as a function of the immutable number and various user parameters (col. 6, lines 6- 39).

7. Claims 16,35 additionally recite the limitation that the scrambling/de-scrambling key be processed from (i.e., a function of) at least, the remote computer number. Chapman clearly processes the remote computer number as one of several key components in creating the scrambling/ descrambling key (figure 3, col. 11, lines 26- 42).

8. Claims 26,29,32,34 differ from claims 1,14 respectively, in that articles and systems, instead of methods are recited. Chapman clearly discloses articles in the form of a system and (embodied) computer program (abstract).

9. Claim 21 additionally recite the limitation that multiple levels of XOR'g is used. The examiner asserts that multiple XOR'g would be an arbitrary choice used to enhance the security and speed of encoding stream data.

Conclusion

10. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:

Application/Control Number: 09/275,911

Page 8

Art Unit: 2136

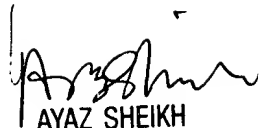
After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7246

Ronald Baum

Patent Examiner


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100